Proceedings of the 4th International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2026.34424

Analysis of Several Issues Concerning the Application of the Crime of Assisting Information Network Criminal Activities through Illegal Quadrilateral Payment Platforms

Ying Zeng

School of Law, Xiamen University Jiageng College, Zhangzhou, China
jnl23058@stu.xujc.com

Abstract. With the development of the digital economy, mobile payment technology has evolved from third-party platform payments to fourth-party platform payments, significantly improving transaction efficiency. Some illegal platforms exploit the operational flexibility of the four-party platform to operate through various mechanisms, making fund settlements covert and rendering comprehensive supervision difficult. This article takes illegal four-party platforms as its focal point. The research analysis reveals that the crime of assisting information network criminal activities exhibits a "pocket-style" characterization. Due to the highly generalized nature of its criminal provisions, for instance, the phrase "serious circumstances" lacks specific elaboration—this leaves room for ambiguity in legal characterization. Meanwhile, the academic community has yet to establish a unified standard for the subjective element of "knowing full well". This leads to issues such as a weakening of subjective "knowledgeful awareness" and irregularities in handling competitive-cooperative scenarios. By reasonably drawing on relevant foreign laws, regulations, and case studies for analysis, this study clarifies the constitutive elements of the offense and delineates its distinctions from other crimes, thereby addressing the issue of the "pocketization" of the crime of aiding information dissemination.

Keywords: crime of assisting information network criminal activities, illegal quadrilateral payment platforms, several issues concerning

1. Introduction

After decades of development, crimes involving illegal four-party payment platforms have evolved from a loose, isolated criminal framework into a mature and comprehensive criminal network. The study found that financial crimes have long attracted attention, whereas certain aspects of internet crime are relatively recent and require in-depth investigation. In examining the research directions of modern financial crime trends, people emphasize the need to identify, thoroughly assess, and study every potential source and tool of financial fraud [1]. The crime in question involves the offense of assisting information network criminal activities. It refers to knowingly knowing that others are using information networks to commit crimes. Providing technical support or assistance with payment settlements. Since 2020, the number of first-instance trials for information technology

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2026.34424

assistance crimes conducted by courts nationwide has increased annually. In the peak year, the volume reac.hed 100,000 units, reflecting a trend toward "portability". The term "pocket crime" is a colloquial designation used by Chinese criminal law scholars to refer to a specific category of offenses. These are charges that can easily be used to cover a wide range of behaviors that are difficult to classify precisely. The original legislative purpose of such charges was to address the complex and ever-changing social circumstances. However, for its ambiguous definition, it is prone to abuse, thereby contradicting its original intent. Placing the authority to interpret the law in the hands of case-handling personnel creates room for selective law enforcement in judicial practice. Some actions that originally constituted civil disputes or public security penalties have been directly escalated into criminal cases, resulting in a mismatch between the severity of the offense and the corresponding punishment. In the illegal four-party payment cases, ambiguous legal characterization is widespread; despite clear presumptive norms and difficulties in verifying fund flows, this results in "difficult convictions, inconsistent sentencing, and weak asset recovery". This makes it more prone to abuse in cases of aiding information dissemination, further exacerbating its tendency toward pocket-like. Regarding illegal quadrilateral platforms, the focus is primarily on regulation and governance. The criminal law research focuses on qualifying offenses such as illegal business operations, aiding information network criminal activities, and concealing or covering up relevant facts.

This article begins by examining the practical operations of illegal four-party payments. Clarifying the relationship and boundaries between this offense and the crime of assisting information network criminal activities. Analyze the manifestations, causes, and regulatory risks associated with the "pocket-like" of this criminal offense. Adopt an international perspective. By comparing the regulatory experiences of regions such as the United States and the European Union regarding similar practices involving "illegal payment intermediaries". Referring to the relevant criminal law theories of Germany and Russia. Propose a precise regulatory approach encompassing three dimensions: the explicit constitutive elements, judicial interpretations, and the boundaries of legal characterization. To balance criminal punishment with the principle of restraint in criminal law, this paper provides theoretical references and practical recommendations.

2. The structure of illegal quadrilateral platform payments and the applicability boundaries of the crime of assisting information network criminal activities

2.1. The applicable logic of the crime of assisting information network criminal activities in illegal four-party platform payments

The fourth platform payment is an aggregated payment, integrating multiple payment interfaces to provide merchants with one-stop payment services without directly clearing funds. Illegal four-party payment platforms evade regulation by relying on formal payment channels to settle illegal funds for criminal activities. Current criminal activities have formed a complete criminal chain, primarily comprising four typical models: bench marking platforms, shell company interfaces, virtual transaction money laundering, and nested aggregation interfaces. The gray supply chain mainly includes three roles: system builders, platform operators, and offline personnel [2].

Article 287-2 of the Criminal Law of the People's Republic of China aims to criminalize "assistance acts" within the internet crime supply chain as an extension of Article 287. From an analysis of its constituent elements and in conjunction with relevant judicial interpretations, "payment settlement" does not refer to all forms of fund flow; in essence, it refers to the transfer of monetary funds through legal settlement methods.

DOI: 10.54254/2753-7048/2026.34424

Specifically, in the illegal four-party platform model, it often disguises itself as a "game company" or "e-commerce platform", defrauds regular third-party payment interfaces, and then builds capital channels without authorization [3]. During this process, the actor's implementation of "subsidiary transfer" cash out, "withdrawal", or "providing facial recognition and other verification services" was clearly identified as a "payment settlement" act under criminal law [4]. When the platform forms "capital precipitation" in the process of capital flow and disposes of itself, it falls within the scope of the crime of aiding information network.

2.2. The characterization of payments on illegal quadrilateral platforms

The crimes involved in illegal fourth platform activities are not limited to assisting in information network crimes; different participants exhibit a clear hierarchical structure in legal application due to differences in the nature of their actions and depth of involvement.

First, the underlying basic crime agents and technical developers constitute the largest group and are the primary subjects responsible for gang crime. The former only provides personal payment accounts, while the latter offers technical support. Both have a general understanding of upstream crimes and typically have no direct connection to them, failing to deeply intervene in financial operations.

For platform operators responsible for executing specific operations such as fund splits and transfers, if their actions exceed the scope of "in-the-middle assistance", they should be deemed guilty of concealing criminal proceeds after upstream crimes are completed.

The platform organizers are the core controllers of the illegal quadrilateral platform, responsible for building the platform architecture, recruiting subscriber numbers, connecting with upstream gambling fraud syndicates, and overseeing fund settlements. The actions often commit multiple offenses simultaneously: for example, operating a payment settlement business without a license constitutes illegal operations; providing payment channels for upstream crimes may be considered a joint crime; and being deeply involved in money laundering is characteristic of money laundering.

Finally, platform providers that have fixed cooperation with criminal gangs and have a clear understanding of upstream crimes due to prior collusion should be deemed accomplices to upstream crimes and subject to more severe statutory penalties.

3. Multidimensional manifestations of the 'pocketing' tendency in the crime of assisting information network criminal activities in illegal quadrilateral platform payments

3.1. Softening of subjective 'knowledge'

In China's theoretical community, the definition of "knowing" can be divided into "knowing", "possibly knowing", and "should know". The first two refer to knowledge that has evidence to prove it, while the latter refers to knowledge that assumes the subjective consciousness of the actor [5].

In the judicial practice of the illegal quadrilateral platform, there has been a softening of the criteria for recognizing "knowledge". Here, softening does not refer to emptiness. Specifically reflected in two aspects:

Knowing that recognition has been alienated from "certain knowledge" to objective behavior presumption clearly lowers the standard of proof. In a telecommunications and internet crime case tried in Xi'an by Yan Liang, Zhai was found by the court to be "knowingly" based not on Zhai's confession, i.e., his confession. Instead, it is inferred from objective abnormal circumstances in reverse. For example, if the transaction price is abnormal, lending two bank cards in this case will

DOI: 10.54254/2753-7048/2026.34424

yield 2,700 yuan, which is significantly higher than the normal rental price; if the transaction is abnormal, it will be delivered specifically from Shanghai to Suzhou; if the channel is abnormal, it will flow through the WeChat Group Help platform.

For the generalization of basic facts about "knowing". In the aforementioned case, the court ruled that "Zhai agreed to lend his bank card despite knowing that it might be used for telecom fraud networks and other criminal activities", thereby generalizing the basic facts and equating "possible knowledge" directly with "knowing". Similar statements include "the actor does not know the other party, which not only provides a foundation of trust", and "the state is actively engaged in anti-fraud activities, so the actor should have a certain understanding of the nature and harm of their actions". [6].

3.2. Overlapping crimes and punishments and lack of uniform standards for handling them

In illegal four-party platform payments, the crime of aiding information network crimes and concealing criminal proceeds often overlap due to multiple offenses committed by the same fund transfer. However, in practice, the distinction between the two becomes blurred, exhibiting multiple instances of misconduct.

The criteria for recognizing "subjective knowledge" vary. If the perpetrator only knows that the other party may be using a card for online gambling or fraud, but is unaware of the specific money laundering method, they are typically convicted of aiding information network crimes; if they clearly know that the funds are "gambling" or "fraudulent", they meet the criteria for concealment. But lower-level personnel often deny knowing about it, and judicial authorities need to rely on objective behavioral inference, with differences in inference standards leading to disagreements in conviction.

Judgment of behavioral intervention time is difficult. Theoretically, providing account receipts before an upstream crime is completed constitutes a crime of aiding information network criminal activities, while assisting in transferring and splitting funds after completion constitutes a crime of concealment. However, the behavior of running errands is intertwined, making it difficult to clearly distinguish them. Different courts focus on different stages, resulting in varying judgments.

"The risk of lenient punishment for serious crimes and severe punishment for minor offenses is prominent." Concealing and concealing crimes is punishable by law, with individuals who have just reached the threshold facing up to three to seven years in prison, whereas those involved in larger-scale information network crimes can be sentenced to up to three years, violating the principle of proportionality.

The criteria for determining amounts are inconsistent. Assistance crimes are calculated based on all processed flows, concealment crimes on substantiating stolen funds, and the selection of sentencing standards for the two crimes when they overlap further exacerbates the inconsistency in judicial application.

4. Causes of the 'pocketing' of information network crime assistance

At the legislative level, the criminal charges for assisting information network criminal activities are described in highly generalized terms. The "Other Assistance" clause, while providing a catch-all provision to address emerging Internet crimes, has sparked controversy over how to characterize the activities of illegal fourth-party payment platforms due to its lack of clear guidelines. The integration of payment interfaces and virtual currency transactions may be classified either as "payment settlement assistance" or fall under the category of illegal business operations. Meanwhile,

DOI: 10.54254/2753-7048/2026.34424

the criteria for determining "knowledgeful intent" and the quantitative indicators for "serious circumstances" have not yet been further refined. In some cases, it is presumed that the perpetrator was aware solely based on abnormal handling fees or transaction volumes. Even omitting the "serious circumstances" requirement in the judgment. All factors can easily lead to inconsistent judgments in similar cases. At the judicial level, such cases are highly concealed, pose challenges in evidence collection, and involve difficulties in subjective verification. Which leads judicial authorities to favor using the crime of assisting information network criminal activities as a catch-all provision. Judicial authorities often rely on the presumption rule to determine whether someone was aware of the facts. Some platforms only provide payment channels without participating in fund settlement, or with minimal involvement, yet are still held accountable for the crime of facilitating information fraud. This reflects a tendency toward the expansion of applicable charges. This expansion has narrowed the scope of application for offenses such as concealment of crimes. Even downgrading actions that should have been classified as accomplices in the upstream chain. It undermines the criminal law's ability to precisely target criminal networks.

5. Reasonable ways to limit the 'pocketing' of internet crime-related information assistance

5.1. Experiences from abroad in regulating illegal payment intermediary activities

Criminals exist in cyberspace, attacking victims around the world [7]. Within a closely interconnected international landscape. Research and draw upon the legal principles and governance approaches of other countries. At the same time, take into account the country's actual circumstances. This helps to more effectively address the tendency toward fragmented or piecemeal approaches in addressing the crime of assisting information network criminal activities.

The German "objective attribution theory" provides important references. German criminal law theory emphasizes that the punishable aiding behavior must be based on a substantial contribution to the infringement of the principal offender's legal interests [8]. In crimes committed on illegal four-party platforms, for the underlying participants who occasionally rent out payment QR codes, a prudent assessment must be made regarding the substantive connection between the act of assistance and the infringement of the legal interests involved in the upstream crime. Avoiding the improper expansion of the scope of application of the crime of aiding information dissemination.

The experience of the United States and the EU in handling payment intermediary behavior at various levels is also worth emulating. They concentrate judicial resources on targeting builders, operators, and primary beneficiaries. For the underlying "code providers", the focus lies on education, administrative penalties, and financial regulation. This strategy that balances leniency with strictness, not only can effectively curb the core aspects of internet crime but also avoid imposing excessive criminal penalties on grassroots participants. In light of China's actual circumstances. The relevant administrative regulations can be further improved. Establishing clear penalty standards for grassroots participants, ensuring a gradual transition between criminal prosecution and administrative penalties.

5.2. Clarifying the connotation of constitutive elements

Regarding the concept of "knowledge", Chinese academia generally advocates for a reasonable limitation of its scope. Most scholars believe that "knowing" in intentional crimes should exclude "should have known", interpreting "knowing" merely as "knowing", and opposing lowering the standard of proof through "should have known" [9, 10]. Accordingly, in crimes involving illegal

DOI: 10.54254/2753-7048/2026.34424

payment platforms, judicial practice must strictly distinguish between "knowing" and "should know".

In China's criminal law system, "knowing" falls under intentional categories, while "should know" falls under negligence. The distinction between the two directly affects the determination of criminal responsibility and sentencing [11]. Current judicial practices blur the lines between the two, with some judgments declaring intent to be "foreseeable" and improperly incorporating negligence, which can lead to objective crime. In judicial interpretations, "presumed knowledge" is an evidence rule rather than an acknowledgment of "should have known", which can be reversed based on objective circumstances such as abnormal transactions or regulatory notifications, but allows the actor to rebut with evidence of fraud or trust. The experience of Russian criminal law also shows that subjective liability determination is highly dependent on careful judgment by investigators, and judicial authorities should handle it with caution [12].

For lower-level salespeople, since they are typically minors or less educated groups, it is assumed that there is a greater difference between their knowledge and genuine knowledge. Only by limiting subjective thinking to "actual knowledge" or "certainty," excluding negligent "should know", can people prevent minor negligence, implement the principle of subject-object alignment, and reasonably limit the application of crimes that aid in information network activities.

At the same time, it helps to achieve a unified understanding of criminal illegality and social harm in the crime of information network activities. According to the principle of criminal law, if a person cannot foresee the criminal nature and harmful consequences of their behavior, they should establish grounds for liability denial. Therefore, judicial recognition must raise the "knowledge" threshold to ensure that actors have a clear understanding of "others using information networks to commit crimes".

5.3. Clarifying the boundaries with other crimes

The crime of aiding information network crimes mentioned above overlaps in conviction with other offenses. Clarifying the distinction between aiding information network crimes and other offenses also helps address the issue of "pocket-like" of such crimes. Starting from the relevant provisions of China's Criminal Law, this analysis examines the elements: the crime of aiding information network crimes involves providing payment channels for upstream crimes, while the crime of concealment targets post-incident actions involving the transfer of criminal proceeds. The crime of assisting in information network criminal activities infringes upon internet security management order, while concealing or concealing criminal proceeds undermines judicial order.

Scholars have noted that by using criminal time, assistance for information network crimes can be categorized as both advanced incidents and in-person support. But from the acts of assistance included in the charge, "advertising promotion" is often carried out during the preparatory phase, "technical assistance" frequently occurs in criminal facts, and "payment settlement" often occurs after the recipient is completed, including statutory "promoting" behaviors that may be interspersed at various points in the crime process [13]. And concealing the crime can only occur after it has been completed. So, when convicting a letter of credit, judgments should still be based on the facts of the perpetrator. During the course of investigation, judicial authorities should distinguish between "payment settlement assistance" and "transfer or whitewashing of illicit funds". In terms of "knowledge", it is clear whether the suspect was aware of aiding illegal activities or of the proceeds of crime. Moreover, it is also necessary to unify sentencing standards, eliminate cases of severe punishment for minor offenses, and ensure that punishments are commensurate. By considering factors such as the subjective malignancy, depth of involvement, and profitability of the perpetrator,

DOI: 10.54254/2753-7048/2026.34424

more scientific and reasonable sentencing guidelines should be formulated to ensure that punishment is commensurate. And standardize the "amount recognition" criteria. Clarify that in cases of competition and cooperation, base sentencing on amounts more consistent with the essence of the crime, unify the criteria for determining amounts in judicial practice, and uphold judicial fairness and unity.

6. Conclusion

The illegal four-party payment platform relies on aggregated payment interfaces and a marking model to settle funds, with clear division of labor in the criminal chain and intersecting behaviors. In prosecuting such covert crimes, the scope of application for information network crimes continues to expand, showing a tendency towards "pocket-like": subjectively, "knowing" and "actually knowing" are blurred, leading to different convictions or even "minor convictions". Legislative summary and judicial pragmatism together shape the dilemma, with "promoting criminal behavior" provisions and "serious circumstances" flexibility providing avenues for expanding charges, while demonstrative dilemmas tend to favor handling crimes related to information networks. For this reason, this paper proposes a triple constraint path: drawing on extraterritorial hierarchical governance experience and German-Russian theory of subjective and administrative punishment; clearly limiting "knowing" to "certainty" or "certainty"; and clarifying the boundaries between crimes and concealment. Only in this way can people return to the original intent of legislating to assist information network criminal activities, achieving a balance between combating crime and protecting human rights.

References

[1] Сигетова, К., Узікова, Л., Доценко, Т. and Бойко, А. (2022). Recent trends in the financial crime of the world. Finansovo-Kredytna Diyal'nist, 5(46), 258-270.
[2] Shang, H., Dong, C. and Li, Y. (2023). The operating model and coping strategies of illegal fourth-party payment platforms. Journal of Wuhan Cadre College, 37(01), 80-84.
[3] Wang, H. (2026). Exposing the 'payment dark web'. Procurator Daily of Shanghai People's Newspaper, 2026-1-03.
[4] Liu, M. (2025). On the concurrent handling of 'payment and settlement' in the 'two cards' case. Procurator Daily of the Supreme People's Procurator of the People's Republic of China, 2025-03-22.
[5] Yang, L. (2026). The trend of pocketing crimes of helping information network criminal activities and its limitation path. Doctoral dissertation, Guilin University of Electronic Technology, Guangxi.
[6] Chen, K. (2026). On the rational return of the determination of 'knowledge' in payment and settlement fraud crimes. Journal of Henan University of Engineering (Social Science Edition), 41(01), 58-63.
[7] Lusthaus, J. (2024). Reconsidering crime and technology: What is this thing we call cybercrime?. Annual Review of Law and Social Science, 4.
[8] Jescheck, H.H. and Weigend, T. (2017). German criminal law. China Legal Publishing House, Beijing.
[9] Zhang, M. (2023). The 'knowledge' in criminal intent. Journal of Shanghai University of Political Science and Law, (01), 38.
[10] Ji, Y. (2022). Simplification and limitation of proof for the crime of assisting information network criminal activities. Legal Review, 40(04), 94.
[11] Bai, X. (2025). Research on the normative boundaries of 'presumed knowledge' in the crime of assisting cybercrime. Journal of Wuhan Metallurgical Management Cadre College, 35(03), 32.
[12] Chebotareva, I.N. (2023). Non-use of subjective rights in Russian criminal proceedings: Causes and consequences. Vestnik Sankt-Peterburgskogo Universiteta - Pravo, 14(03), 629-648.
[13] Sun, D. and Shao, J. (2026). Normative restriction and rule construction of 'assistance in crime' in payment and settlement. Journal of Guizhou University, 44(01), 97.